# Minutes for 5-1-02 WG4 Telecon

### *Participants*

Michael Petri (FAA)
Lee Etnyre (UPS-AT)
Steve Koczo (Collins)
Joel Wichgers (Collins)
Jonathan Hammer (CAASD)
Ganghuai Wang (CAASD)
Andy Zeitlin (CAASD)
Dave Spencer (MIT LL)
Bob Anoll (FAA)
Bob Passman (FAA)
Jerry Anderson (FAA)
Greg Stayton (ACSS)

### *Discussion*

## Introduction / Misc

Jonathan announced that he files and material be sent to him by noon Eastern time on Thursday 5/2, and he will send them to the group in a zip file at that time in preparation for next weeks meeting in Cedar Rapids. We then started into the agenda:

## Common Fault Tree Modules

1) Navigation Fault Tree – Common Module

Suggestions/Comments - Use “Own Ship” and “Other” or “Traffic” as generic terms, rather than “Lead” Aircraft.

Joel: 10-7 is a horizontal integrity limit for WAAS/LAAS and does not include other aircraft integrity issues (e.g., the data bus, other affects of avionics processing of nav data)

Joel: Navigation community did not allocate integrity down to the MOPS levels. Some equipment may not maintain the basic navigation integrity provided by the core navigation

Bob Anoll: GPS MOPS set to 3x10-8 (TSO C-139)

Navigation Fault Tree covers two aspects:

- One bucket is the “signal-in-space”, could include the common mode failure (if all receivers use the same satellites.
    - Other bucket is for aircraft navigation avionics.

What about scaling of 10-7 to 10-9 using different containment bounds

Downscaling is easier to consider, e.g., 10-7 to 10-5.

Exposure time is an issue (per operation – 2 min operation) versus per flight hour (30:1 scale factor).

Signal-in-space is a per hour operation.

Navigation assumes 150 sec per approach .

(Fault Tree tool, can give it a rate value, system life-time versus failure rate, tool does integration)

We will use 10-7 per hour for signal-in-space portion of the fault tree.

SW certification how they translate into failure rates (?)

Andy, we should be doing it the other way around, determine the required failure rate number, then pick the certification level.

Need to determine what nav integrity we really need for our applications, but also tie to realism (available systems)

Joel's IRS comments.

2) Persistent SV Error – Common Module

Incorporates ADS-B system errors.

Eliminate reference to Wake Vortex violation.

Andy – need to elaborate on ADS-B block that this does not include the lead aircraft's navigation error, but consists of other errors induced by ADS-B.

Andy – include TIS-B also in addition to ADS-B

Joel – Comment about single report failure versus a persistent report failure (implementation dependent, fault tree needs to reflect that)

3) Airborne separation violation alert fails – Common Module

ADS-B event includes link failure(s) and ADS-B receive processing failures (we need to break failures down to the level to which we need to make allocations to sub-systems {per ASA MASPS Chapter 2)

Give consideration to the case where multiple aircraft are involved (e.g., CD&R).

We may want to identify the number of basic events (add to agenda for next CR meeting meeting).

Jonathan - "Separation violation algorithm fails to alert in time" is an ASSAP function and may need to be broken down further.

4) Incorrect Target ID – Common Module

Jonathan - Are there application specific aspects to this module?

Luck factor, plausible locations are possible cross-checks

Flight ID failure of transmitting aircraft

Need to capture transmission of wrong flight ID by the target aircraft

Controller reference to ID doesn't match with ID on own display ???

Mitigating circumstances (ID needs to make sense, location needs to be plausible), check should be procedural

Bob Passman – while numbers may not be very good on the fault tree, the cross checks will help considerably.

5) ATC Fails to detect & solve problem – Common Module

Need to have a set structure and a set of numbers for this ATC mitigation.

Dave – Why do we want to breakdown ATC any further?

Jonathan – likes one bubble for ATC. We should be including it in our allocations / fault trees. We should take credit for the ATC contribution(s).

****

Took a Break

****

## Conflict Detection Safety and Hazard Analysis

Table 3 will be added / safety table. Lee is bringing this more in line with the Enhanced Visual Acquisition (EVA) application.

Lee described the Conflict Detection (CD) phase diagram.

Mike P. – is Lee considering the original CD state diagram, which described the alerting system? Should we bring any of this state chart / alerting information into the phase diagram (?). Not sure, but will consider it as appropriate.

Lee then discussed Safety Table for each phase.

Lee - For the high-wing / low-wing landing scenario, where pilot cannot see threatening aircraft depicted on CDTI, Lee noted that ownship aircraft will make a maneuver, but will either first check with ATC, or will perform a visual scan to make sure that the airspace is clear for a maneuver. This is a special case, where the CD CDTI actually motivates the maneuver, but visual scan or ATC contact is still needed to allow the maneuver.

Lee – Will focus on the actual alerting itself, and how they interact with current diagram. PAZ/CAZ alerts, alert boundaries and alert times. Consider adding “PAZ penetration” into the safety table.

Dave – If PAZ penetration alert is late, there may be some loss in response time that one may have had otherwise (?)

Jonathan - In some situation, things could be a little worse in using CD CDTI / alerting, but in many cases CD helps significantly.

Jonathan – pilot could become over reliant on CD CDTI / alerting. May expect to see flashing target on CD CDTI, but it never comes, due to a missed alert.

Lee – If system fails to detect a conflict, you are no worse off if one did not have the capability in the first place. If the CD application gives misleading information, then the concern is to where the system draws the pilots attention. This needs to be considered.

## Chapter 2 and 3 Planning Discussion:

### *ATC Separation Assurance Allocation Assumptions*

Steve Koczo reviewed results from a subgroup meeting of WG4 that addressed the role and contributions of ATC for each of the ASA MASPS applications.

Lee – With respect to the EVAcquistion applications, since ATC callouts of traffic are not mandatory, can we rely on ATC providing traffic advisories, and can we take any credit for it?

Lee – Without transponder codes, ATC does not know how who you are and may not be able to provide call outs.

Bob A. – For the Approach Spacing application, concerning ATC workload decrease, Bob felt that workload would actually increase, requiring greater vigilance from ATC in monitoring aircraft, since they are not providing the speed guidance. Jonathan responded that ATC is not responsible for Wake Vortex separation for this application. ATC is still monitoring for totally outrages / out of wack situations concerning separation between aircraft.

End of Minutes for 5/1/02 Telecon